IT Unit 4

Topic 2

# Information management

**Ch 5, Privacy policies,** p 256

1. What is the purpose of a privacy policy?

Privacy policies is the details about what data is gathered and how it is used and must be included. A privacy policy has information on about how it uses to data collected and to whom it will disclose it.

**Key legislation for storage and disposal of data and information**

1. What is the overall purpose of all the privacy legislation? What general principles does it control?

The laws that govern the collection and use of private information by both government and non-government organisations at both state and federal levels.

1. Who is responsible for implementing the rules and communicating with employees and customers?

Organisations must make employees and customers aware of their rights, as well as their responsibilities, in relation to these laws.

**Privacy Act 1988 amended by the Privacy Amendment (Enhancing Privacy Protection) Bill 2012, came into effect on 12 March 2014.**

1. What is included in the Privacy Act?

Thirteen Australian Privacy Principles (APPs) that apply to the handling of personal information by most Australian and Norfolk Island Government agencies and some private sector organisations, credit reporting provisions that apply to the handling of credit-related personal information that credit providers are permitted to disclose to credit reporting bodies for inclusion on individuals’ credit reports, the collection of storage, use, disclosure, security and disposal of individual’ tax file numbers, the handling of health information for health and medical research purposes in certain circumstances, where researchers are unable to seek individuals’ consent, the information commissioner to approve and register enforceable APPs codes that have been developed and providing a small business operator, who would otherwise not be subject to the Australian Privacy Principles to opt-in to being covered by the APPs.

1. Who is covered under the Privacy Act?

The Privacy Act allows individuals to know why personal information is being collected, how it will be used and who it will be disclosed to, have the option of not being identified, or the use of a pseudonym in certain circumstances, ask for access to personal information, discontinue receiving unwanted direct marketing, ask for personal information that is incorrect to be correct and make a complaint about an entity covered by the Privacy Act, if personal information has been mishandled.

1. Who does the Australian Privacy Principles apply to?

The Australian Privacy Policies generally apply to federal government agencies.

1. List the 13 APP principles.

1) Open and transparent management of personal information. Ensures that APP entitles manage personal information in an open and transparent way. This includes having a clearly expressed and up-to-date APP privacy policy

2) Anonymity and pseudonymity. Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym.

3) Collection of solicited personal information. Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of ‘sensitive’ information.

4) Dealing with unsolicited personal information. Outlines how APP entities must deal with unsolicited personal information

5) Notification of the collection of personal information. Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

6) Use or disclosure of personal information. Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

7) Direct marketing. An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met,

8) Cross-border disclosure of personal information. Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas

9) Adoption, use or disclosure of government related identifiers. Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual

10) Quality of personal information. An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up-to-date and complete. An entity must also take reasonable steps to endure the personal information it uses or discloses is accurate, up-to-date, complete and relevant, having regard to the purpose of the use or disclosure.

11) Security of personal information. An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

12) Access to personal information. Outlines an APP entity’s obligations when an individual request to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

13) Correction of personal information. Outlines an APP entity’s obligations in relation to correcting the personal information it holds about individuals

1. What are the credit reporting principles?

The credit-reporting provisions for consumer credit include the simplification of the language used in reports and improved privacy protections.

1. Elaborate on the application of the Privacy Act.

The Privacy Act applies to both electronic and manual or conventional forms of data gathering and handling by private organisations.

1. What is personal information?

Personal information is defined as being information or an opinion about an identified individual, or an individual who is reasonably identifiable: whether information or opinion is true or not; and whether the information is recorded in a material form or not.

1. What are the penalties for serious and repeated interferences with privacy?

The Act prescribes severe penalties for serious and repeated interferences with privacy which can result in criminal prosecution and or fines of up to $340 000 for individuals and $1 700 000 for public and private organisations.

**Privacy and Data Protection Act 2014**, p 262

1. What groups does the Privacy & Data Collection Act (2014) cover.

The PDPA is intended to strengthen the protection of personal information and other data held by Victorian government agencies including local councils and contractors working for the State Government.

1. What are the 10 information Privacy Principles, (IPPs) involved?

Collection of personal information, use and disclosure of personal information, data quality, data security, openness, access and correction, unique identifiers, anonymity, Transborder data flows and sensitive information

**Health Records Act 2001,** p 263

1. What groups does the Health Records Act (2001) cover.

The Health Records Act protects rights to both living and deceased people.

1. What principles did the Health Records Act create?

Openness, making information available to another health service provider, transfer/closure of practice health service provider and Transborder data flows.

1. What are the privacy principles involved?

Collection, Use and disclosure, data quality, data security and retention, openness, access and correction, identifiers, anonymity, transborder data flows, transfer/closure of practice health service provider and making information available to another health service provider.

1. Under what circumstances may health information be provided to a third party without your consent?

If you are deceased or there is a threat to your health.

1. What is the role of the Health Services Commissioner?

The Health Services Commissioner will try to achieve a resolution by discussion between the parties.

1. Table 5.5 is a summary of the Health Privacy Principles, list these.

Collection, Use and disclosure, data quality, data security and retention, openness, access and correction, identifiers, anonymity, transborder data flows, transfer/closure of practice health service provider and making information available to another health service provider.

**Think about Informatics, 5.8, p 263**. Read the case study and answer the 2 questions:

* 1. Identify key legislation that Stevie should consider before providing the information to the external company.

The use and disclosure of personal information, sensitive information and unique identifiers.

* 1. What are Stevie’s ethical responsibilities to the students, parents and the school?

He must ensure that the information provided is correct, the information will remain confidential and that he is working well with the organisation he decides to work alongside.